Department of Commerce • National Oceanic & Atmospheric Administration • National Weather Service

NATIONAL WEATHER SERVICE Instruction 60-701
November 14, 2003

Information Technology
IT Security

Assignment of Responsibilities

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W. Martin **Certified by:** B. West
Type of Issuance: Initial

SUMMARY OF REVISIONS:

Signed by Barry C. West 10/31/03
Barry C. West Date
Chief Information Officer

1 Introduction 2

2 Definitions. 2
2.1 Classified and Unclassified Systems. 2
2.2 General Support System 2
2.3 Major Application. 2

3 Assignment of Responsibilities 3
3.1 Chief Information Officer 3
3.2 NWS IT Security Officer. 3
3.3 System Owner. 4
3.4 IT System Security Officers (ISSO). 5
3.5 Network and System Administrators (N/SA). 5
3.6 End Users. 6

1 Introduction. The NWS IT Security Program establishes the required framework of security controls that ensure the inclusion of security in the daily operation and management of NWS IT Systems and Resources. The management structure provides a foundation for effectively managing the confidentiality, integrity, and availability of the information and the information systems supporting the mission of the NWS. This Instruction defines the roles and responsibilities specified for all NWS employees (federal and contractor) included in the program management structure.

2 Definitions.

2.1 Classified and Unclassified Systems. A system is considered "classified" if it is used to electronically process, store, or transmit classified data. IT security requirements apply equally to classified and unclassified systems, but the rigor with which controls are implemented is greater for classified systems commensurate with the higher risk associated with classified data.

2.2 General Support System. According to National Institute of Standards and Technology Special Publication 800-18, a General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

2.3 Major Application. According to National Institute of Standards and Technology Special Publication 800-18, a Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

3 Assignment of Responsibilities. The structure for security implementation and administration within NWS is a six layer hierarchy. This instruction establishes the following authorities and responsibilities:

3.1 Chief Information Officer. The NWS Chief Information Officer is responsible to:

3.1.1 Oversee the NWS IT Security Program

3.1.2 Appoint, in writing, an IT Security Officer (ITSO) to implement the IT Security Program within NWS.

3.1.3 Ensure each major subordinate component organization (e.g., FMC) has an appointed ITSO and alternate (These ITSOs will function in a similar manner to the NWS ITSO, with adjustments made for their scope of authority - limited to the subordinate organization only.)

3.1.4 Ensure that all IT Systems and their managers are identified, certified and accredited

3.1.5 Ensure that program official(s) serve as the designated approving authority (DAA) responsible for accrediting each system under their responsibility and for ensuring compliance with system security requirements.

3.2 NWS IT Security Officer (ITSO). The NWS ITSO serves as the central point of contact for the IT Security Program for classified and unclassified systems, and must

3.2.1 Develop and maintain operating unit IT security policy, procedures, standards, and guidance consistent with NOAA, Departmental and Federal requirements;

3.2.2 Ensure that all systems have in place effective security documentation, including a qualitative risk assessment, current IT security plans that accurately reflect system status, annual system self-assessments, current and tested contingency plans, and current certification and accreditation;

3.2.3 Conduct annual self-assessments of the NWS IT Security Program to ensure effective implementation of and compliance with established policies and procedures;

3.2.4 Establish procedures for an IT security awareness and training program for all operating unit personnel, including specialized training as necessary for systems administrators, Contracting Officer's technical Representatives (COTRs), etc.;

3.2.5 Maintain the NWS IT System inventory and provide updated inventories to the NOAA and DOC IT Security Program Managers semi-annually;

3.2.6 Act as the operating unit's central point of contact for all incidents;

3.2.7 Provide information to systems administrators and others concerning risks and potential risks to systems;

3.3 System Owner. System owners have many responsibilities in addition to the day-to-day operation and maintenance of their systems. For classified and unclassified systems under their responsibility, system owners will

3.3.1 Include security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management);

3.3.2 Ensure the security of data and application software residing on their system(s);

3.3.3 Determine and implement an appropriate level of security commensurate with the level of sensitivity of their system;

3.3.4 Develop and maintain security plans and contingency plans for all general support systems and major applications under their responsibility. Plans will document the business associations and dependencies of their system;

3.3.5 Perform risk assessments whenever the level of security on a system or network is modified in order to re-evaluate sensitivity of the system, risks, and mitigation strategies;

3.3.6 Conduct self-assessments of system safeguards and program elements, and ensure certification and accreditation of the system;

3.3.7 Report all incidents to the NWS ITSO and NOAA Computer Incident Response Team (NCIRT);

3.3.8 Ensure system users complete IT security training appropriate to their use of the system;

3.3.9 Ensure IT contracts pertaining to the system include provisions for security;

3.3.10 Ensure systems personnel are properly designated, monitored, and trained, including appointment of an individual to serve as the Information System Security Officer (ISSO), if appropriate (large, complex systems may have a greater need for an ISSO than might a small, simple system).

3.4 Information System Security Officer(s) (ISSO). ISSO's implement system-level security controls and maintain system documentation. Specifically, the ISSO will

3.4.1 Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management);

3.4.2 Assist in the determination of an appropriate level of security commensurate with the level of sensitivity;

3.4.3 Assist in the development and maintenance of security and contingency plans for all general support systems and major applications under their responsibility;

3.4.4 Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies;

3.4.5 Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system;

3.4.6 Report all incidents to the NWS ITSO and NOAA Computer Incident Response Team (NCIRT);

3.4.7 Handle and investigate incidents in cooperation with and under direction of the IT Security Officer;

3.4.8 Participate in vulnerability scanning and penetration testing of systems/networks.

3.5 Network and System Administrators (N/SA). N/SA's are responsible for specific aspects of system security, such as adding and deleting user accounts as authorized by the system owner and normal operations of the system in keeping with job requirements. The N/SA is responsible for implementing DOC, NOAA, and NWS security policies, procedures, and guidelines on local systems and networks. The role of an N/SA may include application administration. The N/SA will

3.5.1 Assist in the development and maintenance of security and contingency plans for all general support systems and major applications under their responsibility;

3.5.2 Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies;

3.5.3 Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system;

3.5.4 Evaluate proposed technical security controls to assure proper integration with other system operations;

3.5.5 Identify requirements for resources needed to effectively implement technical security controls;

3.5.6 Ensure the integrity of technical security controls;

3.5.7 Report all incidents to the NWS ITSO and NOAA Computer Incident Response Team (NCIRT);

3.5.8 Read and understand all applicable training and awareness materials;

3.5.9 Read and understand all applicable use policies or other rules of behavior regarding use or abuse of operating unit IT resources;

3.5.10 Develop system administration and operational procedures and manuals;

3.5.11 Evaluate and develop procedures that assure proper integration of service continuity with other system operations;

3.5.12 Know which systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, etc.);

3.5.13 Know the sensitivity of the data they handle and take appropriate measures to protect it

3.6 End Users. End users' responsibilities center upon being aware of the sensitivity of the information they are responsible for and the proper handling thereof. They are responsible to maintain the integrity of this information. This is especially true of the Internet use policy specifying the end user's responsibility regarding Internet introduction of viruses, spams, and malicious codes, normally introduced into a system by a voluntary act of an end user (e.g., installation of an application, FTP of a file, reading mail, etc.). Prevention policies, therefore, should focus on end user training and awareness. End users will

3.6.1 Read and understand all applicable training and awareness materials;

3.6.2 Read and understand all applicable use policies and other rules of behavior regarding use or abuse of operating unit IT resources;

3.6.3 Know which systems or parts of systems for which they are directly responsible (printer, desktop, etc.);

3.6.4 Know the sensitivity of the data they handle and take appropriate measures to protect it;

3.6.5 Report all incidents to their appropriate system administrator in a timely manner; and

3.6.6 Know and abide by all applicable DOC and operating unit policies and procedures.